IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES
(Attorney Docket No. 16379US01)

In the Application of:

Bond et al.

U.S. Serial No.: 09/720,042

Filed: May 6, 2004

For: SOFTWARE VERIFICATION AND AUTHENTICATION

Examiner: Matthew D. Hoel

Group Art Unit: 3714

Conf. No.: 6856

Customer No.: 23446

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via EFS-Web to the United States Patent and Trademark Office on March 23, 2012.

/Jeffrey B. Huter/
Jeffrey B. Huter
Reg. No. 41,086

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from a Final Action dated July 21, 2011, hereinafter the "Final Action." A Notice of Appeal and a three month extension were filed on January 23, 2012, which extended the shortened statutory period for reply to January 23, 2012. The present Appeal Brief is timely filed within the two month period for reply, which extends to March 23, 2012. The appellant respectfully requests that the Board of Patent Appeals and Interferences, hereinafter the "Board," reverse the final rejection of claims 68-87, 95, 97-100, 102, and 103 of the present application in light of this timely-filed Appeal Brief.

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

Aristocrat Technologies Australia Pty Limited, having a place of business at Building A, Pinnacle Office Park, 85 Epping Road, North Ryde NSW 2113, Australia, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 09559, Frame 0690 in the PTO Assignment Search room. The assignment is to Aristocrat Leisure Industries Pty Limited which has subsequently changed its name to Aristocrat Technologies Australia Pty Limited.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

The appellant is unaware of any related appeals or interferences.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The present application includes pending claims 68-87, 95, 97-100, 102, and 103. Claims 68-87, 95, 97-100, 102, and 103 have been rejected. The appellant identifies rejected claims 68-87, 95, 97-100, 102, and 103 as the claims being appealed. The text of pending claims 68-87, 95, 97-100, 102, and 103 is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The appellant has not amended any claims subsequent to the Final Action.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

Claims 69-74 depend from independent claim 68. Claim 68 recites:

68. A system, comprising:

at least one digital storage medium comprising gaming software;[1]

a gaming machine comprising at least one processor configured to authenticate and execute gaming software of the at least one digital medium;[2] and

an authentication agent apparatus, wherein said authentication agent apparatus is external to said gaming machine[3] and further wherein said authentication agent apparatus is configured to:

transmit an authentication algorithm to said gaming machine, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to authenticate said gaming software;[4]

receive from said gaming machine an outcome of said authentication algorithm applied to said gaming software;[5]

compare said received outcome with an expected outcome;[6] and

authenticate said gaming machine if said received outcome matches said expected outcome.[7]

---

[1] See, e.g., storage media 60 of Figs. 1 and 2 and storage media 228a of Fig. 3.
[2] See, e.g., CPU 12 of Fig. 1, page 8, lines 7-19, page 9, lines 1-5, and page 10, lines 11-16.
[3] See, e.g., external requesting agents 222, 222A-C of Figs. 2 and 3, and page 15, lines 26-29.
[4] See, e.g., requester 222 of Fig. 2 and page 15, line 34 through page 16, line 12.
[5] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 12-18.
[6] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 18-24.

Claims 76-78 depend from independent claim 75. Claim 75 recites:

75. (Previously Presented) A method for authenticating gaming software of at least one digital storage medium[8] in a system including a gaming machine and an external authentication agent apparatus[9], said method comprising:

transmitting an authentication algorithm from said external authentication agent apparatus to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine;[10]

deriving an outcome of said authentication algorithm applied to the gaming software of the at least one digital storage medium by execution of the authentication algorithm by said gaming machine;[11]

receiving with said authentication agent apparatus said outcome from said gaming machine;[12]

comparing with said authentication agent apparatus said outcome with an expected outcome;[13] and

---

[7] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 24-29.

[8] See, e.g., storage media 60 of Figs. 1 and 2 and storage media 228a of Fig. 3.

[9] See, e.g., external requesting agents 222, 222A-C of Figs. 2 and 3, and page 15, lines 26-29.

[10] See, e.g., requester 222 of Fig. 2 and page 15, line 34 through page 16, line 12.

[11] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 12-18, and page 16, lines 12-18.

[12] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 12-18.

[13] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 18-24.

authenticating said gaming machine with the authentication agent apparatus if said outcome matches said expected outcome.[14]

Claim 79 recites:

79. A gaming machine comprising:

a gaming controller;[15] and

a data storage device storing data files of games executed by the gaming controller and data corresponding to a valid verification signature,[16]

wherein the gaming controller comprises an interface for loading data external from said gaming machine to said data storage device,[17] and a processor to process a verification algorithm to derive a verification signature[18] and compare said derived signature to said valid signature,[19] and to process an authentication algorithm received via the interface,[20] and

---

[14] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 24-29.
[15] See, e.g., control system 10 of Fig. 1 and page 8, 20-35.
[16] See, e.g., storage media 60 of Figs. 1 and 2 and storage media 228a of Fig. 3.
[17] See, e.g., interfaces 20, 22, 84 of Fig. 1, page 9, lines 8-11, page 10, lines 4-11, loader 226 of Fig. 2, and page 11, lines 32-34.
[18] See, e.g., CPU 12 of Fig. 1, page 8, lines 7-19, page 9, lines 1-5, and page 10, lines 11-16.
[19] See, e.g., CPU 12 of Fig. 1, page 11 lines 21-34, and page 12 line 36 through page 13, line 20.
[20] See, e.g., authentication interpreter 236 of Fig. 2 and page 16, lines 12-15.

wherein the authentication algorithm comprises a plurality of instructions to be executed by the processor of said gaming machine to authenticate said data files of games.[21]

Claims 81-87 depend from independent claim 80. Claim 80 recites:

80. A method for presenting at least one game to a player at a gaming machine, said method comprising:

storing one or more program files for the at least one game in a digital storage medium;[22]

transmitting via a communication link an authentication algorithm to said gaming machine from an authentication agent apparatus, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to derive an outcome of said one or more program files;[23]

processing said authentication algorithm to derive an outcome of said one or more program files for the at least one game via said gaming machine,[24]

receiving said outcome from said gaming machine,[25]

---

[21] See, e.g., math instructions received from requesters 222A-C and placed in request queue 234, page 16, lines 1-15.

[22] See, e.g., data preparation phase 200 of Fig. 2 and page 11, lines 21 through page 12, line 1.

[23] See, e.g., requester 222 of Fig. 2 and page 15, line 34 through page 16, line 12.

[24] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 12-18, and page 16, lines 12-18.

[25] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 12-18.

comparing said received outcome to one of an authorized outcome stored in said digital storage medium or transmitted with said authentication algorithm to determine whether the one or more program files are authentic,[26] and

presenting said at least one game to the player at the gaming machine if the one or more program files are determined to be authentic.[27]

Claims 97-100, 102, and 103 depend from independent claim 95. Claim 95 recites:

95. A system for monitoring a gaming machine, said system comprising:

an authentication agent apparatus;[28] and

a regulating agent apparatus to monitor at least a portion of said gaming machine,[29]

wherein said regulating agent apparatus generates a request for an authentication agent apparatus,[30] and

wherein said authentication agent apparatus is configured to:

transmit an authentication algorithm to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine to derive an outcome of said

---

[26] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 18-24.

[27] See, e.g., responder agents 242A-C of Fig. 3B, page 16, lines 24-25.

[28] See, e.g., external requesting agents 222, 222A-C of Figs. 2 and 3, and page 15, lines 26-29.

[29] See, e.g., external requesting agents 222, 222A-C of Figs. 2 and 3, and page 16, lines 30-36.

[30] See, e.g., page 16, lines 1-12 which indicate the requester and responder are not necessarily the same apparatus.

authentication algorithm applied to at least said portion of said gamine machine;[31]

receive from said gaming machine an outcome of said authentication algorithm applied to at least said portion of said gaming machine;[32]

compare a received outcome from said authentication algorithm at said gaming machine with an expected outcome;[33] and

authenticate said gaming machine if said received outcome matches said expected outcome.[34]

[31] See, e.g., requester 222 of Fig. 2 and page 15, line 34 through page 16, line 12.
[32] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 12-18.
[33] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 18-24.
[34] See, e.g., responder agents 242A-C of Fig. 3B, page 17, lines 18-29, and page 16, lines 24-29.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(c)(1)(vi))

Claims 68-87, 95, 97-100, 102, and 103 stand rejected under U.S.C. § 103(a) as being unpatentable over US 5,643,086 to Alcorn et al., hereinafter "Alcorn," in view of US 5,539,828 to Davis, hereinafter "Davis, " and US 5,355,413 to Ohno, hereinafter "Ohno."

ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

The Final Action rejected claims 68-87, 95, 97-100, 102, and 103 under U.S.C. § 103(a) as being unpatentable over US 5,643,086 to Alcorn et al., hereinafter "Alcorn," in view of US 5,539,828 to Davis, hereinafter "Davis, " and US 5,355,413 to Ohno, hereinafter "Ohno." Reversal of the present rejection of claims 68-87, 95, 97-100, 102, and 103 and allowance of the pending claims is earnestly solicited in light of the following.

I. Claims 68-74

Each of claims 68-74 is directed to a system comprising, among other things, an authorization agent apparatus configured to "transmit an authentication algorithm to said gaming machine, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to authenticate said gaming software; [and] receive from said gaming machine an outcome of said authentication algorithm applied to said gaming software." The appellant respectfully submits that the proposed combination of Alcorn, Davis, and Ohno does not teach or otherwise render obvious such aspects of claims 68-74.

The appellant respectfully submits that the Final Action appears to misunderstand and/or mischaracterize the operation of the Alcorn device in regard to remotely demanding authentication. The appellant believes such misunderstand/mischaracterization may have resulted in the examiner believing that the Alcorn device is closer in operation to the claimed invention, than the Alcorn device is in fact.

For example on page 12, the Final Action states:

> The examiner believes that Alcorn discloses transmitting a verification algorithm to the gaming machine and receiving the verification algorithm from the gaming machine…. Alcorn teaches that the gaming data and unique signature are stored externally (2:27-32). The game data set is only installed on the gaming machine after authentication (2:45-57), so if the gaming data set is stored externally it must receive a signal from the gaming machine before it is loaded onto the gaming machine. The decryption of Alcorn is done with a public key stored in ROM 29 on the gaming device (3:3-6). The game data set on the network is then installed (3:8-12). This will necessarily require a signal from the gaming machine.

The appellant respectfully disagrees with such assessment. First, the appellant notes that the relied upon section never explicitly state that an apparatus "transmits an authentication algorithm to said gaming machine," or that the apparatus "receive from said gaming machine an outcome of said authentication algorithm applied to said gaming software." Instead, the examiner believes that such aspects must be inherent to the Alcorn system due to the gaming data and unique signature being stored externally. The appellant respectfully submits that the examiner is wrong in such belief. As explained in detail below, not only are such aspects not inherently required by Alcorn, Alcorn explicitly teaches away from an implementation that would include such aspects.

As further evidence that the examiner misunderstands the teachings of Alcorn, the Final Action on page 13 contends:

> The authentication can be conducted locally or externally via a network (4:39-58). This external authentication is used to authenticate ROM 29 in the same manner as ROM 29 authenticates the mass storage unit and the rest of the contents of the gaming machine (8:38-52); in this case the

> authentication program would necessarily be external to the gaming machine. This can be done for example, by the gaming commission (8:54-62), so the gaming machine would receive a verification algorithm from the external source and send it back to the external authentication agent (9:47-58).

The appellant respectfully disagrees with such assessment of Alcorn. In regarding to such network operation, Alcorn merely teaches sending a demand via a network to the gaming machine to cause the gaming machine to initiate its authentication procedure. It's fairly clear, when taken in context, such network demand is merely one of many described manners of triggering the authentication procedure, which is executed locally by the gaming machine. For example, Alcorn indicates that the gaming machine may execute the authentication procedure: (i) each time the game is loaded from the mass storage unit into main memory 13; (ii) in response to the pull of a slot game handle; (iii) in response to the detection of a coin inserted into the gaming machine; (iv) in response to the payout of coins or the issuing of credit; (v) in response to activating a manually operated switch on the gaming machine that is only accessible to authorized persons; and (vi) in response to a demand command generated remotely and transmitted to the gaming machine over a network. See, Alcorn 9:27-57.

At 8:1-26, Alcorn explains the execution of its authentication routine. As is clear from 8:1-26, the authentication routine is executed locally by the gaming machine using only locally stored routines. Furthermore, Alcorn clearly indicates that in order to prevent tampering such routines must be stored in an unalterable ROM 29. See, Alcorn 7:12-14 and 8:26-67. As such, Alcorn provides a clear teaching away from the proposed modification of having an external device provide the authentication routine via the network. Such a modification would thwart Alcorn's protections against unauthorized

change and/or bypassing of the authentication routine, namely, the storing of such routines in unalterable ROM 29.

Moreover, despite the Final Actions contentions on page 14 to the contrary, Alcorn never mentions or otherwise suggests receiving a verification algorithm from an external source (e.g., a gaming commission) and sending the verification algorithm back to the external authentication agent. The appellant appreciates that Alcorn in various paragraphs mentions that an external agent, such as a gaming commission, may authenticate the gaming machine. However, the appellant has found no mention or suggestion in Alcorn that such authentication involves the transfer of an authentication routine from the gaming commission over a network to the gaming machine for execution by the gaming machine in the manner suggested by the Final Action.

In fact, Alcorn at 3:22-33 clearly indicates that authentication of the Alcorn device is conducted in the same way as that now performed in prior art devices: viz. computing the message digest directly from the unalterable read only memory device, and comparing the message digest with the custodial version. It should be appreciated that such a comparison merely requires the custodian (e.g., gaming commission) to maintain a custodial copy of the contents of the read only memory device, compute a message digest from the contents, and compare such message digest to a message digest computed from the read only memory device. The appellant respectfully points out that this same procedure is outline in the Background section of the present application at page 2, lines 24-35. As noted at page 2, lines 24-35, such a process does not require the transfer of authentication routines from the gaming commission to the gaming machine for execution by the gaming machine as the Final Action appears to contend.

Moreover, the remote triggering of the authentication routine from the gaming commission via the network is presumably done to cause the gaming machine to compute the message digest and send the digest to the gaming commission via the network. However, the appellant points out that Alcorn does not appear to explicitly disclose the sending of the digest to the gaming commission via the network. Instead, Alcorn appears to only describe the triggering of the authentication procedure via the network. The actual transfer of the message digest to the gaming commission may occur via different means as such aspect is simply not disclosed. Alternatively, the commission may simply trigger periodic execution of the authentication procedure via the network to ensure the gaming machine is checked at least a minimal amount times.

The Final Action on page 13 also states in regard to the page 14 of the Non-Final Action that:

> [T]he examiner was not saying that Alcorn teaches the transmission of an authentication algorithm. The examiner does believe that the transmission of an authentication algorithm would be a minor modification to Alcorn at the time of invention."

The appellant respectfully submits that the above statement directly contradicts the examiner's statement on page 12 which was "[t]he examiner believes that Alcorn discloses transmitting a verification algorithm to the gaming machine and receiving the verification algorithm from the gaming machine." Such contradictory statements are additional evidence regarding the examiner's general misunderstanding of the present teachings of Alcorn. Moreover, the appellant respectfully points out that such a modification would not be "minor" as contended in the Final Action. Alcorn teaches a very specific manner by which security of the platform is maintained. As noted above, Alcorn indicates that storing the authentication routine in an unalterable ROM 29 is an

important part of it's security measures. The "minor" modification suggested by the examiner would undermine the very security measures put into place by Alcorn.

The appellant respectfully submits that Davis adds very little to the teachings of Alcorn in regard to above discussed aspects of claims 68-74. As noted above, Alcorn teaches that the authentication procedure may be triggered remotely by sending a command over the network. Davis basically teaches the same technique. In particular, a remote agent generates a challenge which results in the device to be verified generating a response. If the response is as expected, the remote agent has verified the device's identity and the remote agent may continue encrypted communications with the device. Otherwise, the remote agent determines that the device's identity can not be verified, and the remote agent discontinues communications with the device. Similar to Alcorn, the remote device in Davis does not send an authentication routine to the device for execution. Instead, the remote device in Davis sends the device to be verified a random challenge and determines whether the appropriate response is received. See, Davis 6:39-7-24.

In order to further address this shortcoming of Alcorn and Davis, the Final Action further cites Ohno. In particular, the Final Action on page 5 contends that Ohno teaches an authentication algorithm transmitted from one device to another. The appellant respectfully disagrees. Ohno does not teach transferring an authentication algorithm from one device to another, but instead teaches transferring encryption algorithms (f'1)(g'2) to IC card 13. The appellant respectfully points out that such encryption algorithms are merely a portion of a larger authentication procedure executed by the IC card 13 and is not the authentication procedure itself. The embodiment relied upon by the Final Action corresponds to Fig. 15 in which step 145 is the authentication process. However, as noted at 8:40-42, the authentication process is

the same authentication operation as that executed in previous embodiments. One such embodiment is depicted in Fig. 4 and another such embodiment is depicted in Fig. 5. Based upon Figs. 4 and 5, its clear that encryption algorithms (f'1)(g'2) are not authentication algorithms as contended, but merely encryption algorithms used by an authentication process.

Furthermore, the appellant points out that Ohno merely authenticates the IC card based upon whether the IC card has an expected authentication code stored in the IC card. The authentication operations shown in Figs. 4 and 5 are not applied to software of the IC card to authenticate such software, let alone, applied to gaming software of the IC card to authenticate such gaming software as required by claims 68-74. Accordingly, Alcorn, Davis, and Ohno in combination fail to teach or otherwise render obvious transferring an authentication algorithm to the gaming machine to be (i) executed by the gaming machine and (ii) applied to gaming software of the gaming machine. Moreover, the appellant further submits that Alcorn teaches away from such a modification of the Alcorn device as Alcorn clearly states that the authentication procedures **must** be stored in the unalterable ROM 29 in order to prevent tampering. Such aspects of Alcorn clearly teach away from modifying the Alcorn device in a manner that results in the Alcorn device receiving such authentication procedures via a network as proposed.

Finally, the appellant wishes to address statements made on page 15. In particular, page 15 states:

> The crux of the matter is that the examiner does not believe that merely transmitting an authentication algorithm from a remote party to a networked gaming device contributes anything patentable over Alcorn, since Alcorn already teaches that the message digest resulting from the hash function used to verify the ROM 29 can be transferred over

> the network back to the casino operator or gaming commission in response to a network-initiated authentication command (3:35-55, 4:49-58, 8:38-52); authentication information, though not a complete algorithm, is already transmitted to the gaming device, the only difference with Alcorn is that the claimed algorithm is a series of instructions.

From the above, the examiner believes it's important or the crux of the matter that Alcorn already teaches that the message digest resulting from the hash function used to verify the ROM 20 can be transferred over the network back to the casino operator or gaming commission in response to a network-initiated authentication command. However, the appellant has reviewed the Alcorn portions (3:35-55, 4:49-58, 8:38-52) and respectfully submits that nothing in those portions supports the notion that the message digest is transferred from the gaming machine over the network back to the casino operator or gaming commission as the Final Action contends. Moreover, the appellant has been unable to locate other portions of Alcorn which support such a notion. Moreover, even if Alcorn taught such a notion, the appellant respectfully submits that transmitting to a gaming machine an algorithm with which to calculate an authentication result is greatly different than merely returning the result of an authentication process calculated based on a fixed algorithm stored in gaming machine. Transmitting an algorithm provides the transmitting entity with another level of assurance since they now control the algorithm being used, thus making it much harder for an unscrupulous entity to return a faked valid result.

For at least one or move of the above reasons, the appellant respectfully submits that the present rejection of claims 68-74 is prefaced on a severely flawed factual foundation. As such, a prima facie case of obviousness has not been established in

regard to claims 68-74. Reversal of the present rejection of claims 68-74 is therefore earnestly solicited.

II. Claims 75-78

Each of claims 75-78 is directed to a method that comprises, among other things, "transmitting an authentication algorithm from said external authentication agent apparatus to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine." The appellant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 75-78. Accordingly, the appellant respectfully requests reversal of the present rejection of claims 75-78 for reasons similar to those presented above in regard to claims 68-74.

III. Claim 79

Claim 79 is directed to a gamine machine comprising, among other things, "a process to … process an authentication algorithm received via the interface, and wherein the authentication algorithm comprises a plurality of instructions to be executed by the processor of said gaming machine to authenticate said data files of games." The appellant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claim 79. Accordingly, the appellant respectfully requests reversal of the present rejection of claims 79 for reasons similar to those presented above in regard to claims 68-74.

IV. Claims 80-87

Each of claims 80-87 is directed to a method that comprises, among other things, "transmitting via a communication link an authentication algorithm to said gaming

machine from an authentication agent apparatus, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to derive an outcome of said one or more program files." Again, the appellant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 80-87. Accordingly, the appellant respectfully requests reversal of the present rejection of claims 80-87 for reasons similar to those presented above in regard to claims 68-74.

V. Claims 95, 97-100, 102, and 103

Each of claims 95, 97-100, 102, and 103 is directed to a system that comprises, among other things, "an authentication agent apparatus … configured to: transmit an authentication algorithm to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine to derive an outcome of said authentication algorithm applied to at least said portion of said gaming machine." Again, the appellant respectfully submits that the reasons presented above in regard to claims 68-74 are generally applicable to the patentability of claims 95, 97-100, 102, and 103. Accordingly, the appellant respectfully requests reversal of the present rejection of claims 95, 97-100, 102, and 103 for reasons similar to those presented above in regard to claims 68-74.

CONCLUSION

For at least the foregoing reasons, the appellant submits that the pending claims are in condition for allowance. Reversal of the examiner's rejection and issuance of a patent on the application are, therefore, respectfully requested.

The Commissioner is hereby authorized to charge additional fees or credit overpayments to the deposit account of McAndrews, Held & Malloy, Account No. 13-0017.

Respectfully submitted,

Date: March 23, 2012

By: /Jeffrey B. Huter/
Jeffrey B. Huter
Reg. No. 41,086
Attorney for the Appellant

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661
(T) 312 775 8000
(F) 312 775 8100

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1-67. (Canceled).

68. (Previously Presented) A system, comprising:

at least one digital storage medium comprising gaming software;

a gaming machine comprising at least one processor configured to authenticate and execute gaming software of the at least one digital medium; and

an authentication agent apparatus, wherein said authentication agent apparatus is external to said gaming machine and further wherein said authentication agent apparatus is configured to:

transmit an authentication algorithm to said gaming machine, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to authenticate said gaming software;

receive from said gaming machine an outcome of said authentication algorithm applied to said gaming software;

compare said received outcome with an expected outcome; and

authenticate said gaming machine if said received outcome matches said expected outcome.

69. (Previously Presented) The system of claim 68, wherein an external agent apparatus

prompts said gaming machine to request and execute said authentication algorithm for said at least one digital medium, and

enrolls said gaming machine when said received outcome matches at least one of a set of predetermined criteria.

70. (Previously Presented) The system of claim 68, wherein execution of said authentication algorithm by said gaming machine is carried out based on at least one of a request of said gaming machine, a request of a player of said gaming machine, a request of an authorized agent, and upon a randomly or periodically scheduled event.

71. (Previously Presented) The system of claim 68, further comprising a data storage device configured to historically store said received outcome.

72. (Previously Presented) The system of claim 68, wherein said at least one processor is further configured to execute a verification algorithm to generate a verification signature of said gaming software.

73. (Previously Presented) The system of claim 68, wherein the at least one processor of the gaming machine is further configured to process said authentication algorithm to determine at least one of corruption of said at least one digital medium and tampering with said at least one digital medium.

74. (Previously Presented) The system of claim 68, wherein said authorization agent apparatus is remote to said gaming machine and coupled to said gaming machine via a communication link for transmission of said authentication algorithm to said gaming machine.

75. (Previously Presented) A method for authenticating gaming software of at least one digital storage medium in a system including a gaming machine and an external authentication agent apparatus, said method comprising:

transmitting an authentication algorithm from said external authentication agent apparatus to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine;

deriving an outcome of said authentication algorithm applied to the gaming software of the at least one digital storage medium by execution of the authentication algorithm by said gaming machine;

receiving with said authentication agent apparatus said outcome from said gaming machine;

comparing with said authentication agent apparatus said outcome with an expected outcome; and

authenticating said gaming machine with the authentication agent apparatus if said outcome matches said expected outcome.

76. (Previously Presented) The method of claim 75, further comprising prompting said gaming machine to execute said authentication algorithm for said at least one digital medium and enrolling said gaming machine when said received outcome matches at least one of a set of predetermined criteria.

77. (Previously Presented) The method of claim 75, further comprising executing said authentication algorithm based on at least one of a request of said gaming machine, a request of a player of said gaming machine, a request of an authorized agent, and upon a randomly or periodically scheduled event.

78. (Previously Presented) The method of claim 75, further comprising storing any received outcome from said gaming machine for recollection thereof.

79. (Previously Presented) A gaming machine comprising:

a gaming controller; and

a data storage device storing data files of games executed by the gaming controller and data corresponding to a valid verification signature,

wherein the gaming controller comprises an interface for loading data external from said gaming machine to said data storage device, and a processor to process a verification algorithm to derive a verification signature and compare said derived signature to said valid signature, and to process an authentication algorithm received via the interface, and

wherein the authentication algorithm comprises a plurality of instructions to be executed by the processor of said gaming machine to authenticate said data files of games.

80. (Previously Presented) A method for presenting at least one game to a player at a gaming machine, said method comprising:

storing one or more program files for the at least one game in a digital storage medium;

transmitting via a communication link an authentication algorithm to said gaming machine from an authentication agent apparatus, the authentication algorithm including at least one instruction arranged for processing by said gaming machine to derive an outcome of said one or more program files;

processing said authentication algorithm to derive an outcome of said one or more program files for the at least one game via said gaming machine,

receiving said outcome from said gaming machine,

comparing said received outcome to one of an authorized outcome stored in said digital storage medium or transmitted with said authentication algorithm to determine whether the one or more program files are authentic, and

presenting said at least one game to the player at the gaming machine if the one or more program files are determined to be authentic.

81. (Previously Presented) The method of claim 80, wherein a player is unable to play said at least one game until said one or more program files are determined to be authentic.

82. (Previously Presented) The method of claim 80, further comprising processing said authentication algorithm in response to the player attempting to execute a game of the at least one game.

83. (Previously Presented) The method of claim 80, further comprising downloading the one or more program files from the digital storage medium to said gaming machine, and

initiating processing of said authentication algorithm in response to downloading the one or more program files to said gaming machine.

84. (Previously Presented) The method of claim 80, further comprising triggering, with an agent apparatus external to said gaming machine, transmission of said authentication algorithm and said one or more program files.

85. (Previously Presented) The method of claim 80, further comprising registering said outcome for an audit.

86. (Previously Presented) The method of claim 80, further comprising transmitting an authentication identifier with said authentication algorithm.

87. (Previously Presented) The method of claim 80, further comprising processing said authentication algorithm for identification of at least one of corruption of said one or more program files stored on said digital storage medium and tampering with said one or more program files stored on said digital storage medium.

88-94. (Canceled).

95. (Previously Presented) A system for monitoring a gaming machine, said system comprising:

an authentication agent apparatus; and

a regulating agent apparatus to monitor at least a portion of said gaming machine,

wherein said regulating agent apparatus generates a request for an authentication agent apparatus, and

wherein said authentication agent apparatus is configured to:

transmit an authentication algorithm to said gaming machine, the authentication algorithm comprising a plurality of instructions to be executed by said gaming machine to derive an outcome of said authentication algorithm applied to at least said portion of said gamine machine;

receive from said gaming machine an outcome of said authentication algorithm applied to at least said portion of said gaming machine;

compare a received outcome from said authentication algorithm at said gaming machine with an expected outcome; and

authenticate said gaming machine if said received outcome matches said expected outcome.

96. (Canceled).

97. (Previously Presented) The system of claim 95, wherein said regulating agent apparatus is located remotely from said gaming machine to remotely monitor at least said portion of said gaming machine.

98. (Previously Presented) The system of claim 95, wherein

said regulating agent apparatus monitors all data stored in a digital storage medium of said gaming machine, and

said authentication agent apparatus authenticates said data stored in said data storage medium of said gaming machine.

99. (Previously Presented) The system of claim 95, wherein said authentication agent apparatus is configured to verify that said gaming machine satisfies local gaming regulations.

100. (Previously Presented) The system of claim 95, wherein said regulating agent apparatus monitors software and peripheral devices of said gaming machine.

101. (Canceled).

102. (Previously Presented) The system of claim 95, wherein said authentication agent apparatus via said received outcome of said authentication algorithm detects tampering or rigging of software within said gaming machine.

103. (Previously Presented) The system of claim 95, wherein said authentication agent apparatus authenticates data stored on a digital storage medium in said gaming machine based upon said received outcome of said authentication algorithm.

EVIDENCE APPENDIX
(37 C.F.R. § 41.37(c)(1)(ix))

None.

RELATED PROCEEDINGS APPENDIX
(37 C.F.R. § 41.37(c)(1)(x))

None.